# United States Senate

WASHINGTON, DC 20510-3203

March 2, 2022

The Honorable Patrick Leahy
Chairman
Senate Appropriations
United States Senate
Washington, DC 20510

The Honorable Richard Shelby
Ranking Member
Senate Appropriations
United States Senate
Washington, D.C. 20510

The Honorable Chris Murphy
Chairman
Senate Appropriations
Subcommittee on Homeland Security
United States Senate
Washington, DC 20510

The Honorable Shelley Moore Capito
Ranking Member
Senate Appropriations
Subcommittee on Homeland Security
United States Senate
Washington, D.C. 20510

Dear Chairmen Leahy and Murphy, and Ranking Members Shelby and Capito,

Thank you for your continued support for the cybersecurity readiness and response activities at the Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency (CISA). As you finalize the Fiscal Year (FY) 2022 funding package, we respectfully request significant, dedicated funding for the Multi-State Information Sharing & Analysis Center (MS-ISAC). We urge you to consider dedicating increased funding beyond the FY21 enacted level of $27.014 million for the MS-ISAC program, which is a successful partnership-based approach to building cybersecurity resilience and coordination between federal, state, and local entities.

Extensive cyberattacks on Ukraine's critical infrastructure underscores the need for continued action to defend our homeland and help protect our allies. The Department of Homeland Security (DHS) recently released its "Shields Up" message recommending, "all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets." DHS outlined the continuing need to change from a reactive to proactive stance. MS-ISAC can play a critical role in this work.

The urgency to have stronger cyber defense can be seen by what is playing out as part of a Russian hybrid approach in Ukraine, in Iranian attacks on Israeli water sanitation facilities, and China's focus on compromising telecommunications and other critical infrastructure around the world. All these cyber events demand that the state and local postures are supported firmly by the federal government to deter and respond to future cyber-attacks. In New York, hackers penetrated the Metropolitan Transportation Authority's computer systems as well as the New York Law Department. Cybersecurity and ransomware threats, especially for state, local, territorial, and tribal governments (SLTTs), have been increasing in volume and magnitude for years and they need assistance to combat this threat and this is another area where MS-ISAC can serve well.

Located in Rensselaer County, NY, the Center for Internet Security (CIS) operates as a 501(c)(3) nonprofit organization to advance cybersecurity readiness and response for public and private sector enterprises and is home to the MS-ISAC. Created in 2002, it plays a paramount role in the prevention of, protection from, response to, identification of, and recovery from cyber-attacks against SLTT governments. In 2010, DHS designated the MS-ISAC as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments as well as Fusion Centers. The MS-ISAC is used by all 56 states and territories and more than 12,500 local governments to receive up-to-date information on, and analysis, of cyber threats. Additionally, CIS houses the Election Infrastructure Information Sharing & Analysis Center (EI-ISAC) which provides election systems professionals with a full cyber-defense suite of hardware, software, and expertise to fend off the threat of foreign interference.

MS-ISAC supports information sharing among SLTTs through a broad range of programs, services, and educational forums. For example, MS-ISAC's 24x7x365 Security Operation Center (SOC) provides early cyber threat warnings, threat advisories, vulnerability identification and mitigation, malware and forensic analysis, automated threat feeds and incident response support. These services enhance situational awareness of SLTT networks across the country, including the national cyber situational awareness prepared by the National Cybersecurity and Communications Integration Center (NCCIC). This collective situational awareness of the overall threat landscape enables the MS-ISAC to better assist all SLTT with threat and migration resources and to use its trusted relationships with SLTTs to ensure a two-way, free flow of information between the SLTTs and DHS.

Additional, dedicated funding for the MS-ISAC would allow for expansion of the 'Albert' Sensors program or development of new tools like "Malicious Domain Blocking and Reporting" (MDBR) and 'Endpoint Detection and Response' (EDR)—critical tools in the fight against cyberattacks of all kinds. Albert is an Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC SOC to provide enhanced monitoring capabilities and notifications of malicious activity. The additional funding would also allow for development and broad deployment to SLTT governments of solutions for SLTTs not covered by Albert such as MDBR and EDR, including protection and detection capabilities as we transition to increased use of encryption in support of the recent Presidential cyber security executive order. Additional dedicated funding for the MS-ISAC would allow for the long-term planning and scaling required so that these systems can be fully implemented for improved coordination and threat response across the whole-of-government.

Finally, CIS is also the home of the Critical Security Controls, the set of internationally recognized prioritized actions that form the foundation of basic cyber hygiene--network defense that has been demonstrated to prevent 80-90% of all known pervasive and dangerous cyberattacks. The Controls act as a blueprint to improve cybersecurity by identifying specific actions to be done in priority order. In order to quickly and more directly fight cyberattacks on our nation's 16 critical infrastructure sectors, CIS would organize and coordinate a public-private partnership cyber defense initiative for DHS's Cybersecurity Infrastructure and Security Agency (CISA) based on the CIS Controls.

Increased, dedicated funding for the MS-ISAC would be one of the most cost-effective and resource-efficient tools that our local governments have against the outsized threat we face today and we urge your support of this request.

Thank you for your consideration of this request.

Sincerely,

Charles E. Schumer
United States Senator

Kirsten Gillibrand
United States Senator

Margaret Wood Hassan
United States Senator